# AI fuels surge in sophisticated online scams, Microsoft warns



Online scams have become increasingly sophisticated due to advancements in artificial intelligence, making it easier and quicker for scammers to deceive unsuspecting individuals. A report from Microsoft reveals the alarming scale of AI-powered scams in recent times. The tech giant intercepted nearly 500 malicious web domains throughout the past year and blocked an estimated 1.6 million bot signup attempts every hour.

Vasu Jakkal, Corporate Vice President of Microsoft Security, highlighted the escalation in cybercrime, telling CBS News Confirmed, "Last year we were tracking 300 unique nation-state and financial crime groups. This year, we're tracking 1,500." This significant rise is largely attributed to generative AI, which has streamlined the creation of fraudulent websites, making it possible for scammers to effectively operate like an assembly line. "You can just buy a kit off the web," Jakkal explained. "Someone builds the malware. Someone builds the infrastructure. Someone hosts the website."

Beyond just facilitating the setup of fraudulent sites, AI technology also enhances the believability of these scams. According to Jakkal, scammers employ generative AI to produce convincing product descriptions, images, reviews, and even influencer videos. This sophisticated social engineering approach tricks shoppers into believing they are browsing legitimate businesses, when in fact, they are ensnared in digital traps.

A common tactic outlined in Microsoft's report involves domain impersonation. Scammers create near-perfect copies of legitimate websites, often changing just a single letter in the address, to deceive consumers into handing over money or personal information.

In response to the growing threat, Microsoft has introduced protective measures within its web browser, Microsoft Edge. New features include typo and domain impersonation protection that alerts users if a website URL appears suspicious or misspelled. The browser also utilises machine learning to proactively block potentially harmful sites before users access them. "We're trying to combat at every place where we see there's a potential of someone being vulnerable to a fraud attempt," Jakkal said, emphasizing the importance of putting checks and balances in place to encourage users to pause and reassess.

Cybersecurity experts have recognised Microsoft's efforts as among the most proactive in the industry. Scott Shackelford, Executive Director at the Center for Applied Cybersecurity Research at Indiana University, praised the company's initiatives but also called for increased collaboration between private firms and public authorities. "Having the backing of big tech as part of this kind of public, private partnership would be a really great way to show that they do take it seriously," Shackelford said.

To help consumers protect themselves, CBS News Confirmed compiled various safety tips for online shopping, including:

* Being cautious of impulse buying triggered by pressure tactics like "limited-time" deals and countdown timers.
* Checking the URL for any spelling mistakes or slight deviations from the legitimate site’s address.
* Avoiding reliance on social media links by independently searching for sites through browsers.
* Scrutinising reviews to identify fake endorsements, such as repetitive phrasing or an unusually large number of five-star ratings.
* Using credit cards for online purchases, which provide an added level of protection by allowing disputes or fraud claims if necessary.

These measures aim to equip online shoppers with knowledge and tools to navigate an increasingly complex digital landscape shaped by AI-driven threats.

Source: [Noah Wire Services](https://www.noahwire.com)

## Bibliography

1. <https://www.windowscentral.com/software-apps/unsurprisingly-cyber-criminals-are-using-ai-to-refine-phishing-attacks> - This article discusses how cybercriminals are leveraging AI to enhance phishing attacks, aligning with the claim that AI advancements have made online scams more sophisticated.
2. <https://www.thehackernews.com/2023/09/microsofts-ai-powered-bing-chat-ads-may.html> - This report highlights how malicious ads within Microsoft's AI-powered Bing Chat are being used to distribute malware, supporting the assertion that AI is facilitating more convincing fraudulent schemes.
3. <https://securitybrief.co.uk/story/ai-powered-scams-surge-online-as-microsoft-blocks-usd-4bn> - This article details Microsoft's efforts in blocking AI-assisted scams, including preventing fraud attempts valued at USD $4 billion, corroborating the claim about the scale of AI-powered scams.
4. <https://www.wired.com/story/microsoft-copilot-phishing-data-extraction/> - This piece explains how Microsoft's Copilot AI system can be manipulated by attackers to automate phishing attacks, illustrating the misuse of AI in creating fraudulent websites and content.
5. <https://timesofindia.indiatimes.com/technology/tech-news/microsoft-uncovers-global-hacking-ring-that-used-ai-for-harmful-content/articleshow/118631408.cms> - This article reports on Microsoft's discovery of a global hacking ring that utilized AI to create harmful content, supporting the claim that AI is being used to produce convincing fraudulent schemes.
6. <https://venturebeat.com/security/microsofts-vasu-jakkal-on-how-genai-is-redefining-cybersecurity/> - This interview with Vasu Jakkal discusses the impact of generative AI on cybersecurity, including the rise in identity-related attacks, aligning with the claim about the escalation in cybercrime due to AI advancements.
7. <https://www.cbsnews.com/news/how-to-spot-ai-online-shopping-scams/> - Please view link - unable to able to access data